

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

ORIGINAL
FILE

ORIGINAL
RECEIVED

DEC 24 1992

In the Matter of)
)
)
Inquiry into Encryption Technology)
for Satellite Cable Programming)

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

PP Docket No. 92-234

SUMMARY OF
COMMENTS
OF
NEWS DATACOM

News Datacom is a wholly-owned subsidiary of the News Corporation, a world-wide leader in media and communications whose operations include, inter alia, Twentieth Century Fox Film Company, Twentieth Television, Fox Broadcasting Company, Fox Television Stations, and a 50% interest in British Sky Broadcasting Ltd. (BSkyB). NDC is a part of News Corporation's New Technology Group, organized to stimulate innovation in the application of advanced technology across the entire range of the company's media and entertainment activities.

Under the technical supervision of Professor Adi Shamir, Professor of Applied Mathematics at the Weizmann Institute in Rehovet, Israel, NDC utilizes the latest academic research in cryptography to produce state-of-the-art solutions to a wide variety of video, voice and data security needs. Among NDC's products is the in-use VideoCrypt™ system: an advanced--and proven--conditional access system for subscription television. VideoCrypt uses "Smart Cards" with a standard ISO interface. The benefits of this architecture include:

- vibrant competition among integrated receiver descrambler (IRD) manufacturers,
- lower consumer costs,
- open competition among smart card vendors,
- enhanced and upgradeable features, and
- excellent security.

Originally developed for Sky Television (Sky), a subsidiary of BSkyB, NDC is now preparing to introduce versions of VideoCrypt and VideoGuard™ to the United States. These products are useable in analog, and, importantly, in compression systems.

NDC's design of the overall system for BSkyB supports the Commission's hope that the use of a standard interface protocol utilizing smart card technology might permit a single IRD to function with multiple encryption systems as the U.S. domestic video market moves into digital transmission and compression. The NDC approach will facilitate competition among programmers, IRD manufacturers and access control providers, driving down costs to consumers. Moreover, such a system will be simple for viewers to use: One smart card used in one IRD can be programmed to support multiple, competing access control systems. It is NDC's intention to bring various versions of VideoCrypt to the United States. And we are committed to (1) the use of an ISO standard (non-proprietary) smart card interface; (2) open architecture; (3) and licensing of NDC smart card technology for vendors who do not wish to develop their own ISO standard compatible cards. NDC's market entry can drastically reduce the cost of IRDs in the U.S., as well as provide a platform for new enhanced video and multi-media services--our United Kingdom experience proves it.

As a general rule, we believe that the Commission's goals for the encryption marketplace can best be achieved through competition. NDC is prepared to play a major role in any future competition. We intend to introduce products for satellite, MMDS, MLDS, and cable reception. We also intend to construct a new authorization center to work with the VideoCrypt system. And, we are exploring a wide range of licensing and manufacturing alliances.

The NDC standard interface approach using smart cards will facilitate the use of more than one service authorization center. Market forces should dictate how many authorization centers evolve. The temptation to regulate should be resisted. This is a rapidly evolving marketplace ill suited to the pace and rigidity of government processes. As the first entrant, General Instrument has earned a strong market position. But, the forces of competition are--ultimately--unstoppable. Any company that relies on proprietary interfaces to maintain its position is particularly susceptible to price competition from open architectures and standard interfaces such as those utilized by NDC.

The good news is that competition in encryption technology is on the way. The NDC VideoCrypt system, proven on BSkyB in the United Kingdom, will soon be introduced into this country. The result will be more choice, improved security, enhanced features and lower consumer costs. In terms of digital compression, NDC proposes that, given an open architecture environment wherein smart cards are used, a single IRD can support multiple access control systems. This will provide tremendous flexibility for the market and, as illustrated by the BSkyB experience, allow for fair and low prices for consumers.

RECEIVED

DEC 24 1992

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)
)
)
Inquiry into Encryption Technology)
for Satellite Cable Programming)

PP Docket No. 92-234

**COMMENTS
OF
NEWS DATACOM**

TABLE OF CONTENTS

	<u>Page</u>
Summary	i
I. Introduction	1
II. News Datacom And Its Technology	2
III. The BSkyB Experience And The Promise of VideoCrypt	4
IV. The Encryption Market Needs Competition Not Regulation	13
V. Conclusion	15
Appendix I	

RECEIVED

DEC 24 1992

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)
)
)
Inquiry into Encryption Technology)
for Satellite Cable Programming)

PP Docket No. 92-234

**COMMENTS
OF
NEWS DATACOM**

To: The Commission

News Datacom (NDC) files the following comments in response to the Notice of Inquiry (Notice) in the above-referenced docket.

I.

Introduction

These comments carry a message of hope and promise. Competition in encryption technology is on the way. Increased choice, improved security, enhanced features and lower consumer prices are realistically achievable without government intervention.

News Datacom is bringing its proven, world class conditional access technology to the U.S. television marketplace. NDC is a part of the same entrepreneurial company that created Fox

Broadcasting and injected much needed competition into network television. We now intend to do the same for subscription television technology.

These comments will:

- Describe NDC and its technology;
- Review the performance of NDC's VideoCrypt™ system in the United Kingdom (with an emphasis on consumer benefits) and;
- Urge reliance upon competition, rather than regulation, in seeking to achieve the Commission's goals.

II.

News DataCom And Its Technology

News Datacom is a wholly-owned subsidiary of the News Corporation, a world-wide leader in media and communications whose operations include, inter alia, Twentieth Century Fox Film Company, Twentieth Television, Fox Broadcasting Company, Fox Television Stations, and a 50% interest in British Sky Broadcasting Ltd. (BSkyB). NDC is a part of News Corporation's New Technology Group, organized to stimulate innovation in the application of advanced technology across the entire range of the company's media and entertainment activities.

Under the technical supervision of Professor Adi Shamir, Professor of Applied Mathematics at the Weizmann Institute in Rehovet, Israel, NDC utilizes the latest academic research in cryptography to produce state-of-the-art solutions to a wide variety of video, voice and data security needs.

In 1977, Professor Shamir, together with Massachusetts Institute of Technology colleagues Professors Rivest and Adelman, developed the first and, so far, only Public Key Encryption system, now known as RSA. In 1986, Professor Shamir and Dr. Amos Fiat created the Fiat-Shamir algorithm, a quantum leap forward from traditional cryptographic schemes. Based on "zero-knowledge proofs," the Fiat-Shamir system generates ultra-fast proofs of identity and digital signatures in electronic messages that cannot be forged. RSA and Fiat-Shamir "zero-knowledge" authentication, along with the more traditional encryption algorithms (DES for example), form the technological foundation for NDC's products.

Among these products is the in-use VideoCrypt system: an advanced--and proven--conditional access system for subscription television. VideoCrypt uses "Smart Cards" with a standard ISO interface. The benefits of this architecture include:

- vibrant competition among integrated receiver descrambler (IRD) manufacturers,

- lower consumer costs,
- open competition among smart card vendors,
- enhanced and upgradeable features, and
- excellent security.

Originally developed for Sky Television (Sky), a subsidiary of BSkyB, NDC is now preparing to introduce versions of VideoCrypt and VideoGuard™ to the United States. These products are useable in analog, and, importantly, in compression systems.

III.

The BSkyB Experience And The Promise of VideoCrypt

NDC's design of the overall system for BSkyB supports the Commission's hope that the use of a standard interface protocol utilizing smart card technology might permit a single IRD to function with multiple encryption systems as the U.S. domestic video market moves into digital transmission and compression. The NDC approach will facilitate competition among programmers, IRD manufacturers and access control providers, driving down costs to consumers. Moreover, such a system will be simple for viewers to use: One smart card used in one IRD can be programmed to support multiple, competing access control systems. It is NDC's intention to bring various versions of VideoCrypt to the United States. And we are committed to (1) the use of an ISO standard (non-proprietary) smart card interface; (2) open

architecture; (3) and licensing of NDC smart card technology for vendors who do not wish to develop their own ISO standard compatible cards. NDC's market entry can drastically reduce the cost of IRDs in the U.S., as well as provide a platform for new enhanced video and multi-media services--our United Kingdom experience proves it.

BSkyB currently offers six channels of satellite-delivered television programming to 3.4 million television households in the United Kingdom, which comprises 16 percent of UK TV households. Since 1989, its programming has been relayed by the Astra medium-powered satellite. About three quarters of its subscribers have individual home dishes, and the remaining quarter are cable or SMATV subscribers. Among BSkyB's channels are a general entertainment service, a 24-hour per day news and public affairs service, a sports channel and three movie channels, two of which are currently offered on a subscription basis. BSkyB's subscription movie channels have over 1.7 million subscribers. All of its program services also carry advertising.

When Sky Television decided to transmit subscription movie channels, it required a secure and flexible scrambling system to ensure that only subscribers would be able to gain access to its programming. Sky's need was more acute than that of most U.S. subscription programming purveyors, as the Astra footprint covers all of Western Europe, and the programming (by contract) was only

to be made available to subscribers in England and Ireland, not to English-speaking audiences in continental Europe. Security, therefore, was essential.

Flexibility also was considered essential; as Sky became operational less than seven months after the project was begun, with decoder production commencing only a few months thereafter, it was difficult to define precisely all of the features that might be required of the system in the future.

A third factor in the calculus was Sky's belief that affordable receiving and decoding equipment would be critical to its success. Many of its potential subscribers already had satellite receivers. The ability to produce an inexpensive decoder that could be installed with any existing satellite receiver or that could be integrated to form an IRD in the future was a business imperative.

Finally, as with any scrambling system, it had to be user friendly and could not degrade picture quality.

Since no existing system met Sky's requirements, the line cut and rotate scrambling technology of Thomson Consumer Electronics was married to the smart card encryption technology of NDC, and VideoCrypt was born. The flexibility of smart card

technology allowed for adaptation to the line cut and rotate scrambling technologies even as it will allow use in compressed (i.e., digital) applications.

A smart card solution was attractive for a variety of reasons. It is simple for the consumer, who has something tangible to confirm that the subscription has been paid and is up to date. The information required to be sent over the air is minimal. Very slow data rates can be used, with a consequential ruggedness of data. The encryption algorithm can be changed at will simply by issuing a new batch of smart cards. Additional features can be introduced to the system when new cards are issued. Other programmers have the option of tiering their services onto the same card, or, alternatively, issuing authorization cards of their own.

VideoCrypt can be thought of as a conventional decoder, with all of the secrets and individuality removed and placed in the smart card. An interesting result of this is that every decoder is identical and contains no secrets that would be damaging to the security of the system if they were discovered. It therefore is not necessary to keep track of who manufactures the decoders and to whom they are sold. So long as a standard interface is used, any authorized card can be used with any decoder. Decoders can be built into satellite receivers, video recorders or television sets without any control requirements from the

programmer. The secrets are all in the card, and this is all that needs to be controlled by the programmer. Furthermore, the smart card determines much of the business behavior of the decoder. Altering the code in the smart card (either by replacement or over-the-air downloading of code) can permit the system to perform business features that may not have been designed at the time the original decoder was manufactured.

Both the lack of intelligence of the decoder and the fact that decoders therefore can be manufactured by competing companies contribute to remarkably inexpensive hardware, particularly in comparison with their U.S. counterparts. The retail price of a satellite IRD can be anywhere between \$700 and \$1500 in the U.S. today, while its counterpart costs between \$260 and \$400 (\$U.S.) in the U.K. Admittedly, this is not quite an apples-to-apples comparison, as present U.S. IRDs are steerable between both C and Ku-band satellites, while IRDs in the United Kingdom are for fixed antennas. Notwithstanding, the price contrast is stunning, and, at a minimum it suggests the potential consumer price benefits to be attained by introducing true competition into the manufacture of IRDs in the U.S.

VideoCrypt's other, more conventional features include ready addressability, accurate access control, enhanced security, tiered programs, multiple languages, pay-per-view, subscriber messaging, and parental blocking controls.

Although every decoder is identical, each smart card is personalized, and the programmer knows to whom each card has been sent. The cards are addressed over the air, and therefore it is possible to send individual messages to each subscriber. The message is addressed to the card rather than to the decoder and is displayed on the screen as a static, flashing or rolling message.

Subscribers continue to receive updated smart cards so long as the subscription is current. Service can be terminated simply by not sending a subscriber a card when the next issue is made. Alternatively, the card can be turned off by an over-the-air transmission addressed to it. Another mechanism of ensuring that subscriptions are current is the use of "positive addressing" whereby cards must be actively reviewed (over-the-air) or they will expire. This prevents a person from removing his or her card and only using it occasionally. It also is possible to send a continuous stream of messages to all decoders, listing all cards that are no longer valid, similar to a credit card "blacklist." If a blacklisted card is inserted into any decoder, the decoder will not accept it. This technique is useful for cards reported lost or stolen. VideoCrypt supports all these methods and provides maximum business flexibility to manage subscribers.

As far as security is concerned, the history of video piracy and theft of intellectual property teaches us that if the product is valuable and expensive, someone will find a way to steal it. If the economics of breaking the code (or the hardware) are prohibitive in comparison with the cost of a legal subscription and any breached security can be quickly and economically repaired, the system will not be attractive to piracy attacks.

It is our philosophy that the decoder should not contain any security that, if divulged, will breach the security of the entire system, thus requiring expensive decoder replacements. It is also our philosophy that multiple "lines of defense" must exist in the decoder and throughout the system. One such critical line of defense uses the Fiat-Shamir zero knowledge algorithm, which allows the decoder to determine if the card inserted in the decoder is valid. This is crucial in stemming any proliferation of cloned cards or devices, yet will not jeopardize system security even if divulged due to its zero knowledge characteristics.

The VideoCrypt smart card uses a special micro-processor, so that it is not easy to read the information stored in the card electronically. It also is very difficult to determine the contents of the card simply by monitoring the data flowing to it from the decoder and returned to the decoder from the card. To determine the secrets of the card, it would be necessary to

dismantle the micro-processor and examine it with a special electron microscope. In most cases, the electron microscope would destroy the charge before the pattern could be determined. To duplicate the card in this manner would be a long and expensive process. And if by any chance a card were copied and distributed, that card easily could be blacklisted and rendered impotent as soon as this were discovered, and a new batch of cards could be sent out to replace it. It also should be noted that use of the Fiat-Shamir zero knowledge algorithm provides substantial protection against using duplicated cards.

An alternative form of attack on the system could be to try to determine by some other means the point at which each line is cut. This characteristic is shared by all cut and rotate systems of scrambling. The VideoCrypt encoder uses special techniques to disguise the cut point. It conceivably could be attacked by trial and error, until a decoded picture is seen. This would have to be done in real time, would require very fast and expensive computers and only would decode the picture for the viewer concerned. Therefore, it need not be regarded as a serious threat to the integrity of the existing VideoCrypt system.

A diagram of the VideoCrypt system is attached as Appendix I. At the transmission point, an encoder is used that has the ability to cut and rotate each line of the television picture at

a point determined by the information fed into it. The location of these cut points is, of course, the secret of the scrambling method. This information is fed to the encoder by a PC, the Security Encoder Computer, using a card reader and smart card. This PC can accept input from the Security Database Computer, which acts as an interface to the Subscriber Management System and the program scheduling system. The Security Encoder Computer generates packets of data, including program identification and scheduling information, together with a random number. These packets of data are fed to the smart card, which processes them through a secret algorithm to produce a seed for a Pseudo Random Bit Sequencer (PRBS). This produces a string of eight-bit numbers, which determine the cut point for each line. The packets of information fed to the card also are transmitted over the air. There are no secrets in this information. The decoder extracts these data packets, and feeds them to the smart card in the decoder, which contains the same algorithms as the smart card in the encoder. The same seed is therefore produced, and a similar PRBS reproduces the same cut points, allowing the decoder to cut the lines in the same place as the encoder did and reconstitute the picture.

The data transmitted over the air are not secret and change every few seconds. It is the combination of these data and the information in the cards that provides the decoding information.

Unlike other encryption systems, no keys are transmitted. If this data is tampered with in any way, the picture will not be decoded.

In sum, VideoCrypt is a proven technology that has been successful in the United Kingdom and can be successful in advancing the goals of the Commission's inquiry. Our approach of using a smart card as an active security device, as opposed to a passive device that just stores keys, produces tremendous business and technological flexibility for its users. It offers ease of implementation in compression applications as well as for more traditional uses.

IV.

The Encryption Market Needs Competition, Not Regulation

NDC expresses no opinion regarding the apparent dispute between General Instrument and Titan. But, as a general proposition, we believe that the Commission's goals for the encryption marketplace can best be achieved through competition. And, NDC is prepared to play a major role in any future competition. We intend to introduce products for satellite, MMDS, MLDS, and cable reception. We also intend to construct a new authorization center to work with the VideoCrypt system. And, we are exploring a wide range of licensing and manufacturing alliances.

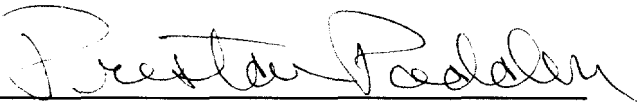
The NDC standard interface approach using smart cards will facilitate the use of more than one service authorization center. Market forces should dictate how many authorization centers evolve. Multiple centers will not increase security risks. Software is available to enhance security at one or multiple authorization centers. Furthermore, assuming piracy will continue to be directed towards decoders, the use of smart cards will allow for an easy change out of a system that is compromised. More importantly, if one of the competing access control systems suffers from repeated successful attacks, the market can move away from that system if installed IRDs can support multiple access systems. Smart cards, as opposed to IRD modules, can be exchanged as consumers move to programming with a different access control system.

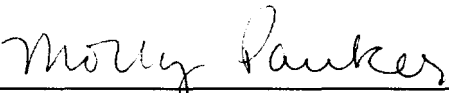
The temptation to regulate should be resisted. This is a rapidly evolving marketplace ill suited to the pace and rigidity of government processes. As the first entrant, General Instrument has earned a strong market position. But, the forces of competition are--ultimately--unstoppable. Any company that relies on proprietary interfaces to maintain its position is particularly susceptible to price competition from open architectures and standard interfaces such as those utilized by NDC.

Conclusion

The good news is that competition in encryption technology is on the way. The NDC VideoCrypt system, proven on BSkyB in the United Kingdom, will soon be introduced into this country. The result will be more choice, improved security, enhanced features and lower consumer costs. In terms of digital compression, NDC proposes that, given an open architecture environment wherein smart cards are used, a single IRD can support multiple access control systems. This will provide tremendous flexibility for the market and, as illustrated by the BSkyB experience, allow for fair and low prices for consumers.

Respectfully submitted,


Preston Padden, Esq.


Molly Pauker, Esq.

5151 Wisconsin Avenue, N.W.
Washington, D.C. 20016
(202) 895-3088

For News Datacom Inc.

Technical Consultants:

Douglas Lindquist
Senior Vice President
Sales & Marketing North America

Norman Reinhardt
Vice President
Business Development North America

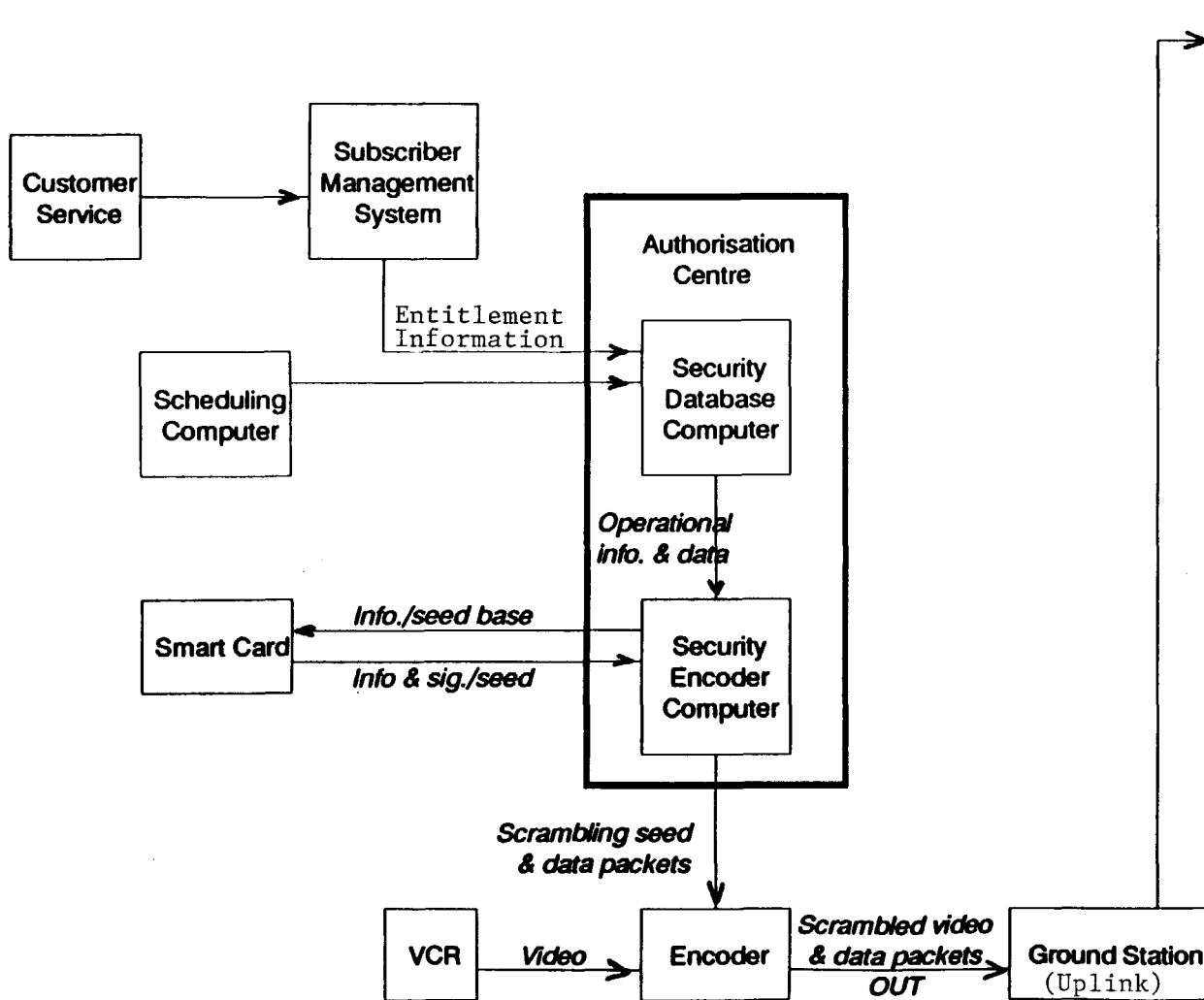
News Datacom Inc.
1430 O'Brien Drive Suite F
Menlo Park, California 94025
(415) 617-0275

December 24, 1992

THE VIDEOCRYPT SYSTEM

(Satellite direct to home example)

TRANSMISSION



RECEPTION

